EXPRESS MAIL LABEL NO. EL377527410US FILING DATE: March 23, 2001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT
(UTILITY PATENT)

Docket No.: 13230-101

APPLICANT: Jayme Matthew Fishman
Larry Powers

POST OFFICE ADDRESS: Powerfish, Inc.
4-302 Greenbriar Drive
North Reading, MA 01864

INVENTION TITLE: SYSTEM AND PROCESS FOR CONDUCTING AUTHENTICATED TRANSACTIONS ONLINE

ASSIGNEE:

Powerfish, Inc.,
a Delaware Corp.
4-302 Greenbriar Drive
North Reading, MA 01864

ATTORNEYS:
Stephen Y. Chow (Reg. No. 31,338)
Christine M. Kuta, (Reg. No. 38,001)
Jerry Cohen (Reg. No. 20,522)
Harvey Kaye* (Reg. No. 18,978)
Jacob N. Erlich (Reg. No. 24,338)
Perkins, Smith & Cohen, LLP
One Beacon Street
Boston, Massachusetts 02108
(617) 854-4000
* Mr. Kaye is available at 301-948-5535

TO: Honorable Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

Your applicant(s), named above hereby petition(s for) grant of a utility patent to him(them) or any assignee(s) of record, at the time of issuance, for an invention more particularly described in the following specification and claims, with the accompanying drawings, verified by the accompanying Declaration and entitled:

SYSTEM AND PROCESS FOR CONDUCTING AUTHENTICATED TRANSACTIONS ONLINE

Field of the Invention

1 The invention relates generally to transactions conducted over a communications network that require authentication of a party to the transaction.

Background of the Invention

2 There is need in an open communication network such as the Internet to provide authentication of transaction parties for a variety of reasons, including, without limitation, assurance of authorization to access certain information, the establishment of a legal contract between the parties, and assurance of creditworthiness of one of the parties. Systems implemented and proposed to provide authentication with various levels of confidence have focused on payment mechanisms.

3 In part because financial institution regulations in the United States have afforded some limitation of consumer liability for fraudulent use of credit cards, secure payment systems employing devices such as "smart cards" with embedded microprocessors, that require special readers (and writers), have not enjoyed popularity in the United States. One alternative proposed, for example by NYCE, is the use of a truncated CD (compact disk) cards, cut roughly to the shape and size of a credit card to allow use in conventional desktop and mobile computers and transportation in a wallet. "One-use" tokens of alphanumeric strings may be written on these CD cards, read on a consumer's desktop or mobile computer and transmitted to the issuer of the token for authentication of the token.

4 This system focuses on the authentication of the token rather than the identity of the holder of the CD card. While this may be adequate for payment systems analogous to the carrying of cash, there are many network transactions that require identification of a party to the transaction to determine authority, age, etc.

5 Generally identification of a party to a transaction has been performed using passwords or personal identification numbers (PINs) bound to a user name. These pieces of information are susceptible to diversion. In transactions that require high levels of security, such as administration of a certification authority in a digital signature system, smart cards with encrypted keys have been used in conjunction with logging in with a user name and password. This typically done within a certification authority facility and does not address the need for identification. Identification in currently implemented digital signature systems relies on the possession of the transaction party of a "private key" of an asymmetric private-public-key pair. Various schemes including certification and registration authorities are defined using the asymmetric keys under ANSI's X.9 standard. As these keys typically are kept on a desktop or mobile computer, however, the identification really is of a person (or electronic agent) having access to the keys on that computer. Encryption of the keys on the computer with the use of a password to unlock the keys for each transaction remains cumbersome.

6 Multiple security methods have been combined for different purposes. An example is provided in U.S. Patent No 5,485,519, entitled "Enhanced Security for a Secure Token Code," issued to Weiss, which discloses a method and apparatus for enhancing the

security for a private key by combining a PIN or other secret code memorized by the user with a secure token code to generate a meaningless multi-bit sequence stored in the token. This particular method is viewed as too complex for many of the day-to-day transactions that require authentication of the identity of a party.

7 There is a need for a portable identification device carried by ordinary people (as consumers, employees or non-specialized professionals) that is usable with ordinary computers (such as desktop or notebook computers) that will not be usable if the device is lost or stolen.

Summary of the Invention

8 The instant invention solves this problem by providing encrypted information on a truncated CD card that in some relevant portion is matched against a data base, including information associated with the user to be identified, by an authentication service provider (a "trusted third party") in response to the transmission to that service provider of information personally known only to the user ("personal code"), such as a password. The CD card may fit in an ordinary wallet and be read on the CD- or DVD-drive of an ordinary desktop or mobile computer, concentrating processing at the service provider and thereby minimizing cost to the user and the user's transaction partner, in turn facilitating broad day-to-day use. Because the encrypted information residing on the CD card and the personal code resident in the mind of the user are transmitted to the service provider in close temporal proximity, there is assurance against diversion of authenticating information.

9 In one embodiment, the encrypted information on the CD card are "one-use" tokens implemented as unique sequences of alphanumeric characters embedded among other alphanumeric characters, a portion of which is transmitted to the authorization service provider for matching to a user identified by the personal code; these may be applied as unique signatures to transactions or documents memorializing transactions. In another embodiment, the encrypted information is a digital certificate that is transmitted to the service provider for matching. Other security methods may be added easily to improve on the overall security.

Brief Description of the Drawings

10 Fig. 1 shows schematically the system and process of one implementation of the invention.

11 Fig. 2 shows schematically the system and process of an alternative implementation of the invention.

Detailed Description of a Preferred Embodiment

12 Fig 1 shows an implementation where the party requiring authentication (authentication-seeking entity or "ASE") collects both the CD-resident identifying encrypted information and the personal code for transmission to the communicates with the authentication service provider. A user at terminal 10 (which, without limitation, may be a desktop or notebook computer at home, at work or at a point-of-sale-or-service kiosk) accesses 1 the web page 21 of the other transaction party, which may reside on ASE computer 20 (which, without limitation be a desktop, workstation or institutional

mainframe computer), which prompts 2 for identification of the user. The user inserts into user terminal 10 CD card 11 with encrypted one-use tokens or a digital certificate (these may be "CDR cards", which may be written using ordinary "CD burners"). The user enters password 3 (which may be any personal code known personally only to the user and, for authentication purposes, to the authenticating entity), which is transmitted 4 along with an encrypted token from CD card 11 (the user name or similar identification, known to the ASE, may be transmitted at the same time or may have been provided previously upon logging in). This information is then transmitted by the ASE in a query 5 to trusted third party (TTP) servers 30, one of which may decrypt the CD card information and compares 6 the derived key information for matching on the authenticating entity's preexisting data base with the user password. If there is no match, there may be further prompting and termination of the transaction if the appropriate password is not transmitted. The authentication results are returned 7 to the ASE..

13 Fig 2 shows an alternative implementation where the ASE collects only the CD-resident identifying encrypted information, which may serve as a signature, and the personal code is transmitted by the user to the authentication service provider, limiting the possibility of diversion of the personal code by the ASE. A user at terminal 10 accesses 1 the web page 21 of the other transaction party. ASE computer 20 prompts 2 for identification. The user inserts into user terminal 10 CD card 11 with encrypted one-use tokens or a digital certificate. The user then enters the password 3, which is

transmitted 4' to TTP servers 30. An encrypted token from CD card 11 has been or is transmitted 4 to ASE terminal 20 and forwarded in a query 5 to TTP servers 30, which compare 6 the derived key information for matching with the user password. If there is no match, there may be further prompting and termination of the transaction if the appropriate password is not transmitted. The authentication results are returned 7 to the ASE.

14 In either implementation, the token or digital certificate may serve as a signature associated with the transaction or documentation of the transaction. Records of the transaction with date-stamps may be kept by the authentication service provider with little burden on the user or the ASE.

15 The system and process may be integrated into desktop applications as plug-in modules or separate application programs. For example, transaction parties may negotiate a contract by exchanging "red-lined" revisions, and upon agreement (or a "milestone" in a "rolling contract" that continues to evolve), one party may invoke the authentication system and process, for example, by clicking a button in a toolbar or printing to the authentication application. The authentication application would prompt for insertion of the party's authentication key, that is, the information (tokens or certificates) resident on the CD card. Once the key is inserted and the user code (password) entered, the party's "signature" is applied; this may simply be a token that can be matched to the user by the authentication service provider (TTP). In this application,

each transaction party (and there may be more than two) may act as an ASE for the other transaction parties. Alternatively, there may be no ASE at all, but the authentication service provider or TTP would be a registry for signing or authentication events established by the transmission to it directly (and matching) of the CD-resident information and the personal code, with different possibilities for the TTP's archiving of document- or transaction-identification information, copies of signed documents, unique digital "hashes", etc.

16 It should be understood that the authentication service provider (TTP) in each of the embodiments described above may be owned by the same legal entity that owns the ASE and may be on the same local network, as may be the user terminal. Thus, the invention may be usefully applied to identification of users on corporate intranets.

17 It should also be understood that in each of the embodiments described above, various security/authority levels may be assigned to different authentication keys (tokens or certificates) or personal codes or combinations thereof.

18 Finally, while the embodiments described here rely upon the use of two security devices, namely, unique information resident on a wallet-sized storage device, and unique information personally known only to the user, particular implementations may apply other security devices, or factors, including the user name (such as logging in to an ASE web site), location (such as origination from a node on a particular local network), future biometrics (handwritten signatures, fingerprints, voice, etc.) or combinations of the above to provide even higher levels of assurance of proper authentication.